

证 明

本证明之附件是向本局提交的下列专利申请副本

申 请 日： 2002 09 23

申 请 号： 02 1 42880.8

申 请 类 别： 发明

发明创造名称： 有条件接收系统中的密钥分配方法及装置

申 请 人： 国际商业机器公司

发明人或设计人：张健；刘宗伟；邵凌；谢东

中华人民共和国
国家知识产权局局长

王 景 川

2003 年 2 月 9 日

权 利 要 求 书

1. 一种有条件接收系统中的密钥分配方法, 假设该系统所能容纳的全部用户节点的集合为全集, 由全部用户节点或其中部分用户节点构成一子集合, 其特征在于包括下列步骤:
- 5 (1) 将所述子集合分解为至少一个次级子集合;
- (2) 为各次级子集合分配不同的用户密钥, 所述各用户密钥被传送给对应次级子集合中的所有用户;
- (3) 使用各所述用户密钥加密一授权密钥以生成对应于各个次级子集合的各密码文本;
- 10 (4) 将所述密码文本组合生成媒体密钥控制块。
2. 如权利要求 1 所述的密钥分配方法, 其特征在于所述方法还包括步骤: 将所述媒体密钥控制块发送给所述子集合中的所有用户。
3. 如权利要求 1 所述的密钥分配方法, 其特征在于: 其中一视频节目
- 15 是使用所述授权密钥加密的。
4. 如权利要求 1 所述的密钥分配方法, 其特征在于: 其中一控制字是使用所述授权密钥加密的, 而一视频节目是用所述控制字加密的。
5. 如权利要求 3 或 4 所述的密钥分配方法, 其特征在于: 每个次级子集合中的用户从所述媒体密钥控制块识别出所属次级子集合的所述密码文本, 并用自身的用户密钥解密, 以取得所述授权密钥。
- 20 6. 如权利要求 1—4 中任一所述的密钥分配方法, 其特征在于: 所述媒体密钥控制块可以在广播信道上单向发送。
7. 如权利要求 1—4 中任一所述的密钥分配方法, 其特征在于: 所述经分解的次级子集合在所述系统建立后可以保持不变。
- 25 8. 如权利要求 1—4 中任一所述的密钥分配方法, 其特征在于: 用二叉树算法将所述子集合分解为所述至少一个次级子集合。
9. 如权利要求 1—4 中任一所述的密钥分配方法, 其特征在于: 使用多叉树算法将所述子集合分解为所述至少一个次级子集合。
10. 一种在有条件接收系统中使用的密钥分配装置, 假设该系统所能容纳的全部用户节点的集合为全集, 由全部用户节点或其中部分用户节点构成一子集合, 其特征在于所述密钥分配装置包括:
- 30

- 分解单元，用于将所述子集合分解为至少一个次级子集合，并为各次级子集合分配不同的用户密钥，所述各用户密钥被传送给对应次级子集合中的所有用户；
- 生成单元，用于使用各所述用户密钥加密一授权密钥以生成对应于各个次级子集合的各密码文本；
- 组合单元，用于将所述各密码文本组合生成一媒体密钥控制块；和
- 授权控制装置，用于控制所述各个单元的相应操作并输出所述媒体密钥控制块。
11. 如权利要求 10 所述的密钥分配装置，其特征在于还包括发送装置，用于将从所述授权控制装置接收的所述媒体密钥控制块发送给所述子集合中的所有用户。
12. 一种用于有条件接收系统中的发送设备，假设该有条件接收系统所能容纳的全部用户节点的集合为全集，由全部用户节点或其中部分用户节点构成一子集合，其特征在于所述发送设备包括：
- 15 分解单元，用于将所述子集合分解为至少一个次级子集合，并为各次级子集合分配不同的用户密钥，所述各用户密钥被传送给对应次级子集合中的所有用户；
- 生成单元，用于使用各所述用户密钥加密一授权密钥以生成对应于各个次级子集合的各密码文本；
- 20 组合单元，用于将所述各密码文本组合生成一媒体密钥控制块；
- 节目加扰单元，用于使用所述授权密钥加扰一视频节目；
- 发送单元，用于将经加扰的视频节目和所述媒体密钥控制块发送给一接收设备；和
- 授权控制装置，用于控制所述各个单元的相应操作并将所述媒体密钥控制块输出给所述发送单元。
- 25 13. 如权利要求 12 所述的发送设备，其特征在于：所述发送设备还包括控制字加密单元，用于在所述授权控制装置的控制下，使用所述授权密钥将一控制字加密为所述密码文本，其中所述节目加扰单元用所述控制字加密所述视频节目。
- 30 14. 如权利要求 13 所述的发送设备，其特征在于：所述密码文本是权利控制消息（ECM）。

15. 如权利要求 12 至 13 中任一所述的发送设备, 其特征在于: 所述分解单元使用二叉树算法将所述子集合分解为所述至少一个次级子集合。

16. 如权利要求 12 至 13 中任一所述的发送设备, 其特征在于: 所述分解单元使用多叉树算法将所述子集合分解为所述至少一个次级子集合。

5 17. 如权利要求 12 至 13 中任一所述的发送设备, 其特征在于: 所述授权控制装置还用于管理用户信息。

18. 一种用于有条件接收系统中的接收设备, 假设该有条件接收系统所能容纳的全部用户节点的集合为全集, 由全部用户节点或其中部分用户节点构成一子集合, 其特征在于所述接收设备包括:

10 接收单元, 用于接收从发送设备发送的经加扰的视频节目和媒体密钥控制块;

解析单元, 用于使用用户密钥解密一密码文本以获得一授权密钥; 其中所述密码文本是使用与该接收设备所属的次级子集合相对应的用户密钥对所述媒体密钥块进行识别获得的, 所述次级子集合是将所述子集合分解而成
15 的;

节目解扰单元, 用于使用所述授权密钥解密经加扰的视频节目。

19. 如权利要求 18 所述的接收设备, 其特征在于: 所述接收设备还包括控制字解密单元, 用于使用所述授权密钥解密所述密码文本以获得一控制字, 其中所述节目解扰单元用所述控制字解扰所述视频节目。

20 20. 如权利要求 19 所述的接收设备, 其特征在于: 所述密码文本是权利控制消息 (ECM)。

有条件接收系统中的密钥分配方法及装置

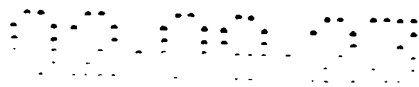
5 技术领域

本发明涉及有条件接收系统，更具体地涉及在有条件接收系统中分配密钥的方法和设备。

背景技术

- 10 有条件接收 (conditional access, CA) 系统对于有线/卫星付费电视广播商来说是非常重要的，而有条件接收系统中最重要的是如何向系统中自动地添加合法用户 (已付费用户) 和从系统中移除非法用户，其基本结构是 EMM (权利管理消息) → ECM (权利控制消息) → CW (控制字) → 流 (Stream)。如图 1 所示，运营商 (发送侧) 通过网络广播向每个合法用户播发 EMM 和 ECM，
- 15 该 EMM 中含有要传达给每个用户 (接收侧) 的一条信息，该信息中包含用户所需要的授权密钥 MK，每个用户的设备在接收该 EMM 的时候对其进行过滤，一旦获得要传送给该用户的、EMM 中的那条消息，就利用事先从运营商处获得的
- 20 用户密钥 (以智能卡或其它方式分发给用户) 将该条消息解密以获得其中的授权密钥 MK，然后再用该授权密钥 MK 解密 ECM 以获得 CW，而这个 CW 是用来加密视频流 (例如 MPEG-2) 的。这样，合法用户就可以通过运营商向其动态分配的授权密钥 MK 而观看加密的视频节目了，而未付费的用户 (非法用户) 则由于不能获得该授权密钥 MK 而不能观看加密的视频节目。

- 在这个 CA 系统中，EMM 扮演了一个分配该授权密钥的重要角色。但不幸的是，在大多数 CA 系统中，EMM 的长度都很长。一般地，该长度与这个 CA
- 25 系统中的用户的数量成正比，在很大的系统中，它可能会变得非常的庞大。由于这个长度很大，广播这个 EMM 就会占用更大的带宽，有时为了接收 EMM，人们还不得不打开他们的机顶盒 (set-top box)。由于 MPEG-2 的 TS 流允许将多个码流组合在一起，EMM 和 ECM 并非由单独的信道进行发送，而是与视频流同时传递的，同时在一一般情况下，EMM 每月变化一次，而 ECM 每十秒钟
- 30 变化一次，所以它们在发送时所占用的带宽会严重影响视频节目的接收和观看。这种情况使得诸如 PPV (Pay Per View, 接收看付费)、IPPV (Impulsive



Pay Per View, 即时接收看付费) 和准 VOD (视频点播) 变得非常不方便。例如, 在一个拥有 10000 名用户的常规 CA 系统中, 如果有 1% 的用户 (100 名用户) 想离开这个系统, 则该系统就必须向剩下的 9900 名用户中的每一个用户发送含有其中每个用户信息的 EMM, 以通知他们改变他们的组及其所

5 拥有的原授权密钥 MK。这样, 广播这些通知就占用了大量的带宽, 浪费了大量的资源。

发明内容

为了解决上述问题, 本发明的目的是提供一种在有条件接收系统中的密钥分配方法和装置, 该方法是将合法用户按一定的条件分割为不同的组, 为

10 每组中的用户分配相同的用户密钥, 从而多个用户可以用该相同的用户密钥来获得授权密钥 MK。

为了达到上述目的, 本发明提供了一种有条件接收系统中的密钥分配方法, 假设该系统所能容纳的全部用户节点的集合为全集, 由全部用户节点或

15 其中部分用户节点构成一子集合, 其中包括下列步骤: 将所述子集合分解为至少一个次级子集合; 为各次级子集合分配不同的用户密钥, 所述各用户密钥被传送给对应次级子集合中的所有用户; 使用各所述用户密钥加密一授权密钥以生成对应于各个次级子集合的各密码文本; 将所述密码文本组合生成一媒体密钥控制块。

20 其中使用二叉树算法将所述子集合分解为所述至少一个次级子集合。

本发明还提供了一种在有条件接收系统中使用的密钥分配装置, 假设该系统所能容纳的全部用户节点的集合为全集, 由全部用户节点或其中部分用户节点构成一子集合, 其中所述密钥分配装置包括: 分解单元, 用于将所述子集合分解为至少一个次级子集合, 并为各次级子集合分配不同的用户密

25 钥, 所述各用户密钥被传送给对应次级子集合中的所有用户; 生成单元, 用于使用各所述用户密钥加密一授权密钥以生成对应于各个次级子集合的各密码文本; 组合单元, 用于将所述各密码文本组合生成一媒体密钥控制块; 和授权控制装置, 用于控制所述各个单元的相应操作并输出所述媒体密钥控制块。

30 本发明还提供了一种用于有条件接收系统中的发送设备, 假设该有条件接收系统所能容纳的全部用户节点的集合为全集, 由全部用户节点或其中部

分用户节点构成一子集合，其中所述发送设备包括：分解单元，用于将所述子集合分解为至少一个次级子集合，并为各次级子集合分配不同的用户密钥，所述各用户密钥被传送给对应次级子集合中的所有用户；生成单元，用于使用各所述用户密钥加密一授权密钥以生成对应于各个次级子集合的各密码文本；组合单元，用于将所述各密码文本组合生成一媒体密钥控制块；节目加扰单元，用于使用所述授权密钥加扰一视频节目；发送单元，用于将经加扰的视频节目和所述媒体密钥控制块发送给一接收设备；和授权控制装置，用于控制所述各个单元的相应操作并将所述媒体密钥控制块输出给所述发送单元。

- 10 本发明还提供了一种用于有条件接收系统中的接收设备，假设该有条件接收系统所能容纳的全部用户节点的集合为全集，由全部用户节点或其中部分用户节点构成一子集合，其中所述接收设备包括：接收单元，用于接收从发送设备发送的经加扰的视频节目和媒体密钥控制块；解析单元，用于使用用户密钥解密一密码文本以获得一授权密钥；其中所述密码文本是使用与该接收设备所属的次级子集合相对应的用户密钥对所述媒体密钥块进行识别获得的，所述次级子集合是将所述子集合分解而成的；节目解扰单元，用于使用所述授权密钥解密经加扰的视频节目。

- 15 由于本发明使用了二叉树分类方法，同组中的多个用户可以共用一条消息来获得授权密钥 MK，从而减少了用于分配该授权密钥 MK 的 EMM（本发明中为 MKCB）的信息量（长度），使 MKCB 的长度大大短于常规的线性管理，特别是在用户离开系统的时候。因此，本发明可以节省广播 EMM 时所占用的大量带宽，即可以节省大量的网络资源。

附图说明

- 25 本发明的上述和其它目的和优点将在下面结合附图和具体实施例对本发明的进一步说明中变得更加清楚，其中：

图 1 是常规的有条件接收系统中的发送端和接收端的示意图；

图 2 是根据本发明在有条件接收系统中使用的密钥分配装置的结构图；

图 3 是根据本发明在有条件接收系统中使用的密钥分配方法的流程图；

- 30 图 4 是根据本发明一实施例在有条件接收系统中使用的视频节目发送设备的结构图；

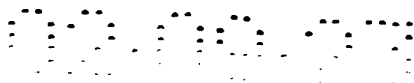


图 5 是根据本发明一实施例在有条件接收系统中使用的视频节目接收设备的结构图；

图 6 是根据本发明另一实施例在有条件接收系统中使用的视频节目发送设备的结构图；

5 图 7 是根据本发明另一实施例在有条件接收系统中使用的视频节目接收设备的结构图；

图 8 是示例 n 阶二叉树算法的图；

图 9 是进一步示例 n 阶二叉树算法的图。

10 具体实施方式

下面将结合附图和具体实施例对本发明进行详细地说明。

媒体密钥控制块 (MKCB) 的定义和特征

本发明的 MKCB 方法可以用来实现有条件接收系统中的 EMM 层。

15 假设所有用户或用户设备 (节点) 的集合是全集 I (即系统所能容纳的所有用户), S 是 I 的一个子集, 表示已经注册的合法用户 (例如是已经付费的用户)。在本发明中, 采用二叉树算法 (后面将更详细地进行说明) 将子集合 S 分解为多个次级子集合 $D1$ 、 $D2$ 、...、 Dn , 并且为该多个次级子集合分配不同的用户密钥, 而每个次级子集合中的用户具有相同的用户密钥。然后用各个不同的用户密钥分别将授权密钥加密成密码文本 $E1$ 、 $E2$ 、... En ,
20 并将上述密码文本组合生成本发明的媒体密钥控制块 $MKCB(S, MK)$, 这个 $MKCB(S, MK)$ 中的授权密钥 MK 可以用来将指定的视频节目的控制字 CW 加密成 ECM , 该控制字 CW 是用来加密上述视频节目的。当然, 上述的视频节目也可以直接使用该授权密钥 MK 来进行加密, 在这种情况下, 就不用控制字来加密该视频节目了。

25 在 MKCB 的实现方法中, 还可以使用三叉树算法或多叉树算法将子集合 S 分解为多个次级子集合。在本发明的实施例中, 使用二叉树算法来实现, 这将在后面进行详细地描述。当使用这种二叉树算法来实现 MKCB 时, 由于将传统的对用户的线性管理改变为分组管理, 所以 MKCB 的长度不与子集合 S 中的用户数量的增长成线性正比, 并且在大多数情况下非常短。

30 有条件接收系统中生成和分配 MKCB 的装置和方法

图 2 是根据本发明在有条件接收系统中使用的密钥分配装置 1 的结构

图。

如图 2 所示,本发明在有条件接收系统中使用的密钥分配装置 100 包括:分解单元 102,用于将子集合 S 分解为至少一个次级子集合 D_i ,并为各次级子集合分配不同的用户密钥 K_i ,各用户密钥 K_i 被传送给与该密钥对应的次级子集合中的所有用户(可通过智能卡等形式);生成单元 104,用于使用各用户密钥 K_i 加密一授权密钥 MK,以生成对应于各个次级子集合的各密码文本 E_i ;组合单元 106,用于将各密码文本 E_i 组合生成一媒体密钥控制块 MKCB;和授权控制装置 108,用于控制上述各个单元的相应的操作并输出所述媒体密钥控制块。另外,授权控制单元 108 还可以用于管理用户信息,即可以在该媒体密钥控制块 MKCB 中包括运营商要发送给用户的其它用户管理信息。

其中,该分解单元 102 采用二叉树算法将子集合 S 分解为多个次级子集合 D_1 、 D_2 、...、 D_n ,为多个次级子集合 D_1 、 D_2 、...、 D_n 分配不同的用户密钥,和用所述各用户密钥加密所述授权密钥 MK,并将加密授权密钥后所获得的密码文本 E_1 、 E_2 、...、 E_n 进行组合,以生成本发明的媒体密钥控制块 $MKCB = \{E_1, E_2, \dots, E_n\}$ 。

本发明的上述密钥分配装置可以在视频/音频广播的有条件接收系统的单向信道上发送媒体密钥控制块 MKCB,对各用户节点进行单向管理。另外,本发明中分解单元 102 采用二叉树方法所分成的多个次级子集合 D_1 、 D_2 、...、 D_n ,在系统建立时一经确定,就可以在以后的使用中保持不变(除非需要改变系统,诸如改变系统的容量等时)。这样,就避免了进行动态管理而带来的繁重的工作量,也节省了进行动态交互管理所需要的大量网络带宽。

该 MKCB 可以在指定节目开始前广播给合法用户,也可以随着节目一起广播,由于其长度较短,其广播的时间和方式是很灵活的。

图 3 是图 2 中的在有条件接收系统中使用的密钥分配装置的工作流程图。如图 3 所示,在步骤 S10,分解单元 102 将全集 I 中的一子集合 S 分解为至少一个次级子集合 D_1 、 D_2 、...、 D_n ;并为上述各次级子集合分配不同的用户密钥 K_i (步骤 S20),所述各用户密钥 K_i 被传送给与该用户密钥相对应的次级子集合中的所有用户;在步骤 S30,生成单元 104 使用各所述用户密钥 K_i 加密一授权密钥 MK,以生成对应于各个次级子集合的各密码文本 E_i (即 E_1 、 E_2 、...、 E_n);在步骤 S40,组合单元 106 将所述密码文本 E_i 组合生成

一媒体密钥控制块 $MKCB = \{E1, E2, \dots, En\}$ 。另外在步骤 S50, 所生成的媒体密钥控制块 MKCB 通过授权控制装置 108 输出, 并经一发送单元发送给予集合 S 中的所有用户。

下面将对使用本发明图 2 中密钥分配装置的视频节目发送设备进行详细地说明, 其中与图 2 中的密钥分配装置相同的部件采用相同的附图标记, 并且为了简单起见, 将省略对其相同功能的描述。

图 4 是根据本发明一实施例在有条件接收系统中使用的视频节目发送设备 100 的结构图。

如图 4 所示, 视频发送设备 100 包括: 分解单元 102, 生成单元 104, 组合单元 106, 和授权控制单元 108, 这些单元与图 2 中所示的相同单元具有相同的功能和结构; 除此之外, 视频发送设备 100 还包括: 节目加扰单元 110, 用于使用授权密钥 MK 加扰来自一视频节目生成装置 (未示出) 的源码流 (视频节目); 发送单元 112, 用于将经加扰的视频节目和该媒体密钥控制块发送给一接收设备 200 (如图 5 所示)。

下面将结合附图对本发明中的视频节目接收设备 200 进行详细地说明。

图 5 是根据本发明一实施例在有条件接收系统中使用的视频节目接收设备 200 的结构图。

如图 5 所示, 视频节目接收设备 200 包括: 接收单元 204, 用于接收从发送设备 100 发送的经加扰的视频节目和媒体密钥控制块; 解析单元 202, 用于对所述媒体密钥块 MKCB 进行识别, 以获得与该接收设备 200 所属的次级子集合 Di 相对应的密码文本 Ei (即 $E1, E2, \dots, En$ 之一), 并使用与该次级子集合 Di 相对应的用户密钥 Ki 解密该密码文本 Ei , 以获得一授权密钥 MK; 节目解扰单元 206, 用于使用所获得的授权密钥 MK 解密经加扰的视频节目, 并将经解扰的视频节目传送给如电视等的接收或回放设备进行接收或回放。

当然, 解析单元 202 还可以用于管理用户信息, 其在解密 MKCB 后可以获得由运营商发送给用户的信息, 并将其发送给其它设备 (未示出) 进行存档或进行其它处理。

这里, 对于包含所有可容纳用户节点的全集 I 的任何给定的合法用户子集 S, $MKCB(S, MK)$ 中的授权密钥 MK 可以且仅可以由子集合 S 中的用户解密, 而该 MK 是用来加密 MPEG 视频流的, 这样, 子集合 S 中的用户 (合法付

费的用户)在解密 MKCB 并获得 MK 后,就可以再进一步获得经解扰的 MPEG 视频流。

下面将结合附图 6 说明本发明的视频发送设备的另一个实施例,其中与图 4 中的视频发送设备相同的单元采用相同的附图标记,并且为了简单起见,将省略对其相同功能的描述。

图 6 是根据本发明另一实施例在有条件接收系统中使用的视频节目发送设备 300 的结构图。

如图 6 所示,视频发送设备 300 包括:分解单元 102,生成单元 104,组合单元 106,授权控制单元 108,和发送单元 112,这些单元与图 4 中所示的相同单元具有相同的功能和结构,不再进行描述;除此之外,视频发送设备 300 还包括:控制字加密单元 114,用于在授权控制装置 108 的控制下,使用授权密钥 MK 将一控制字 CW 加密成上述的密码文本 Ei。

与视频发送设备 100 的不同之处还在于:本实施例中视频发送设备 300 的节目加扰单元 110 用于使用控制字 CW 加密来自一视频节目生成装置(未示出)的源码流(视频节目),生成经加扰的视频节目。这里的密码文本 Ei 就是有条件接收系统中的权利控制消息(ECM)。下面将结合附图 7 说明本发明的视频接收设备的另一个实施例,其中与图 5 中的视频接收设备 200 相同的单元采用相同的附图标记,并且为了简单起见,将省略对其相同功能的描述。

图 7 是根据本发明另一实施例在有条件接收系统中使用的视频节目接收设备 400 的结构图。

如图 7 所示,视频节目接收设备 400 包括:接收单元 204,解析单元 202,这些单元与图 5 中所示的相同单元具有相同的功能和结构,不再进行描述;除此之外,视频发送设备 300 还包括:控制字解密单元 208,用于使用从解析单元 202 输出的、经解密的授权密钥 MK 解密与该接收设备 400 对应的密码文本 Ei(属于该用户的 E1、E2、...、En 之一,即 ECM),以获得所述控制字 CW。

与视频接收设备 200 的不同之处还在于:本实施例中视频接收设备 400 的节目解扰单元 206 使用所述控制字 CW 解密经加扰的视频节目,并将经解扰的视频节目传送给如电视等的接收或回放设备进行接收或回放。

这里,对于包含所有可容纳用户节点的全集 I 的任何给定的合法用户子

集 S , $MKCB(S, MK)$ 中的授权密钥 MK 可以且仅可以由子集合 S 中的用户解密。该 MK 用来将 CW (控制字) 加密为 ECM (权利控制消息), 而 CW 是用来加扰 MPEG 视频流的。这样, 子集合 S 中的用户 (合法付费的用户) 在解密 $MKCB$ 并获得 MK 后, 就可以通过用 MK 解密 ECM 而获得 CW , 从而再进一步获得经解扰的 MPEG 视频流。

5 用二叉树算法生成 MKCB 的实例

下面结合图 8 和图 9 说明利用 n 阶二叉树算法生成 MKCB 的实例。

如图 8 所示, 假设一个完整的 n 阶二叉树。很清楚, 在该树中有 $2^n - 1$ 个节点, 其中包括一个根节点和 2^{n-1} 个叶节点。所谓叶节点, 是指没有子节点的节点, 即树的最“下”层。另外, 每个节点都可以看作是某一子树的根节点, 该子树包括该节点本身和所有它的后代节点, 是与该节点对应的子树。我们可以使每个节点与其对应的子树相关, 例如, 根节点与整个树相关, 叶节点与仅包括该节点本身的该级子树相关。在图 8 中, 节点 1 表示与节点 a 相关的子树, 节点 2 表示与节点 v 相关的子树。

如图 8 所示, 子树差 $D'(u, v)$ 是子树差节点的集合, 子树差节点可以通过两个节点 u 和 v 来识别, 这里 v 是 u 的后代节点。如果用 $T'(u)$ 表示与节点 u 对应的子树, 用 $T'(v)$ 表示与节点 v 对应的子树, 那么子树差 $D'(u, v)$ 包括属于 u 子树但不属于 v 子树的所有节点, 它可以看作是与节点 u 相关的子树减去与节点 v 相关的子树, 即 $D'(u, v) = T'(u) - T'(v)$ 。在图 8 中, 节点 3 表示通过子树差 $D'(u, v)$ 所识别的子树。

在本发明的这种算法中, 设全集 I 是所有叶节点的集合, 即图 8 中由点划线所包围部分中的所有节点。也就是说, 每个叶节点表示一个用户, 因此这种算法中用户的最大数目是 2^{n-1} 。

如图 9 所示, 假定 S 是 I 的子集, 可以证明存在一定数量的子集差 $D(u, v)$, 它们的和是子集合 S 。或者说, S 可以被拆分为多个子集差 $D(u, v)$ 。这里所述的子集差 $D(u, v)$ 是指子树差 $D'(u, v)$ 中所有叶节点的集合。图 9 示出了子集合 S 的拆分情况, 这里, 子集合 S 包括所有带标号的叶节点。如图 9 所示, 子集合 S 是各个子集差 $D(u_1, v_1)$ 、 $D(u_2, v_2)$ 、 $D(u_3, v_3)$ 和 $D(u_4, v_4)$ 的和。其中子集差 $D(u_1, v_1) = T(u_1) - T(v_1)$ 、 $D(u_2, v_2) = T(u_2) - T(v_2)$ 、 $D(u_3, v_3) = T(u_3) - T(v_3)$ 和 $D(u_4, v_4) = T(u_4) - T(v_4)$ 。这里, $T(u)$ 表示 $T'(u)$ 中所有叶节点的集合, $T(v)$ 表示 $T'(v)$ 中所有叶节点的集合。

对于每个子集差 $D(u, v)$ ，都有一个分配给它的密码值 $K(u, v)$ （即用户密钥），这个密码值 $K(u, v)$ 必须分配给该 $D(u, v)$ 内的所有用户。对于不属于 $D(u, v)$ 的任何用户，密码值 $K(u, v)$ 必须是未知的和不可计算的。

假设媒体密钥控制块 MKCB 是 $E(K(u, v), MK)$ 的和，这里 $E(K(u, v), MK)$ 表示在每个子集差 $D(u, v)$ 中使用 $K(u, v)$ 作为用户密钥来加密授权密钥 MK 所得到的密码文本。那么，这个 MKCB 只能由具有这些 $K(u, v)$ 之一的用户进行解密。也就是说，能够解密 MKCB 的用户属于这些子集差 $D(u, v)$ 之一。由于这些子集差的和构成了子集合 S，因此，仅仅是子集合 S 中的用户可以获得 MK。

下面举例说明媒体密钥控制块 MKCB 的构成。

如图 9 所示，假设合法用户子集合 S 可以拆分为 4 个子集差 $D(u_1, v_1)$ 、 $D(u_2, v_2)$ 、 $D(u_3, v_3)$ 和 $D(u_4, v_4)$ ，那么就要分别为子集差 $D(u_1, v_1)$ 中的用户分配密码值 K_1 ，为子集差 $D(u_2, v_2)$ 中的用户分配密码值 K_2 ，为子集差 $D(u_3, v_3)$ 中的用户分配密码值 K_3 ，和为子集差 $D(u_4, v_4)$ 中的用户分配密码值 K_4 。并且，用密码值 K_1 加密授权密钥 MK 可以获得其密码文本 E_1 ，用密码值 K_2 加密授权密钥 MK 可以获得其密码文本 E_2 ，用密码值 K_3 加密授权密钥 MK 可以获得其密码文本 E_3 ，用密码值 K_4 加密授权密钥 MK 可以获得其密码文本 E_4 。由上述可知，媒体密钥控制块 $MKCB = \{E_1, E_2, E_3, E_4\}$ 。

这样，当用户的接收设备接收到该 MKCB 时，就对该 MKCB 中的信息进行过滤和识别。识别的方法例如可以为 MKCB 中的每个密码文本 E_1 、 E_2 、 E_3 、和 E_4 分配各自的标识，或将每个密码文本 E_1 、 E_2 、 E_3 、和 E_4 分别放置在 MKCB 中具有相应标识的位置，在每个子集差 $D(u, v)$ 中的用户设备检测具有与其自身相对应的标识的密码文本，或检测在 MKCB 中具有与其自身相对应的标识的位置处的密码文本，进行解密。即，属于子集差 $D(u_1, v_1)$ 中的用户检测 MKCB 中含有 E_1 的信息，并用其所拥有的密码值 K_1 将该 E_1 解密，从而获得 MK；属于子集差 $D(u_2, v_2)$ 中的用户检测 MKCB 中含有 E_2 的信息，并用其所拥有的密码值 K_2 将该 E_2 解密，从而获得 MK；属于子集差 $D(u_3, v_3)$ 中的用户检测 MKCB 中含有 E_3 的信息，并用其所拥有的密码值 K_3 将该 E_3 解密，从而获得 MK；属于子集差 $D(u_4, v_4)$ 中的用户检测 MKCB 中含有 E_4 的信息，并用其所拥有的密码值 K_4 将该 E_4 解密，从而获得 MK。

由此可知，有且只有构成了合法用户子集合 S 的子集差之一中的用户可以获得 MK。

每个用户需要存储的用户密钥的数量问题

在常规的方法中，对于每个用户，其必须存储（或可推导计算）子集合 S 中包含其自身的所有子集差 $D(u, v)$ 所对应的密码值 $K(u, v)$ （用户密钥）。这些用户密钥即是由运营商分配给合法用户（例如已交费的用户）的，用来解密运营商所广播发送的本发明中的 MKCB，以获得观看加密的电视节目所必需的授权密钥 MK。这些用户密钥例如可以被存储于智能卡中。

经过简单的数学计算就可以知道，对 n 阶二叉树而言，包含某个叶节点的子集差是 $2^n - n - 1$ 个，同 2^n 是一个数量级的，即 $O(2^n)$ 。当 n 比较小时，即子集差的数量较小时，可以采取直接存储的方法，也就是将数量较小的这些用户密钥直接存储于例如智能卡中；但是在 n 较大时，子集差的数量呈几何级数增长，将变得非常的大，这时要分配或存储如此庞大数量的子集差将会是很困难的事情。

在本发明中，当 n 比较大或者存储空间比较有限时，可以用下面的方法来压缩密钥空间：

在对每个子集差 $D(u, v)$ 赋予 $K(u, v)$ 时，使用这样的算法：

(1) 如果 u 是 v 的父节点，那么直接赋予一个随机密钥（或用其它方法推导也可以）；

(2) 如果 u 不是 v 的父节点， v 的父节点是 v_f ，那么在 $K(u, v_f)$ 给定的情况下， $K(u, v)$ 可以用一个单向强函数从 $K(u, v_f)$ 计算得到。

所谓的单向强函数是加密算法中一个常用的概念，它是这样的：可以从一个数值用一定的方法简单地计算出另一个数值，但是要想从被计算出的数值推导回原始的数值却非常困难，即在函数 $y=f(x)$ 中，由于已知函数关系，从 x 计算得到 y 是容易的，但是由于不知道其逆函数的关系，因此要想从 y 计算出 x 却是非常的困难。

容易看出，这是一个收敛的递归算法。本发明在采用这样的算法后，每个用户就不需要存储包含其自身的所有子集差 $D(u, v)$ 所对应的 $K(u, v)$ 了，因为大部分 $K(u, v)$ 可以从其它 $K(u, v)$ 中推导出来。不难验算，此时每个用户仅需要存储 $n(n-1)/2$ 个密钥，与 $n^2/2$ 是一个数量级，即 $O(n^2/2)$ ，而不是与 2^n 具有相同数量级，因此所要存储的用户密钥的数量大大减小了。而由于单向强函数的性质，可以看到这时整个系统的安全性也并没有降低。

子集合 S 中的子集差的划分

当一个用户由于加入该系统而占用一个节点时，对于该系统而言，该用户的位置也就固定了。该位置相对于整个系统，其所对应的所有子集差 $D(u, v)$ 的情况也是固定的，所有子集差 $D(u, v)$ 的划分情况及其所对应的密码值 $K(u, v)$ 都通过相应的程序存储在系统的数据库（未示出）中。

另外，运营商通过例如上面所述的智能卡的形式将包括该节点的所有子集差 $D(u, v)$ 所对应的密码值 $K(u, v)$ （用户密钥）分配给该节点位置的用户。这样，当某个用户加入或离开子集合 S 时，系统自动计算出在该用户加入或离开后子集合 S 中对应于该情况的各个子集差 $D(u, v)$ ，并将由该各个子集差 $D(u, v)$ 中的密码值 $K(u, v)$ 加密授权密钥 MK 所形成的媒体密钥控制块 $MKCB$ 广播发送给每个用户。由于每个位置的用户都具有对应于改变后的各个子集差 $D(u, v)$ 的 $K(u, v)$ ，因此他们都可以不受影响地解密该媒体密钥控制块 $MKCB$ 而获得授权密钥 MK 。

用 $MKCB$ 方法增加和移除用户

在容量未滿的系统中，还有未被用户使用的空余节点。如果将一个新的用户加入到这个系统中，他/她就会占用这个节点，并得到一组对应于该节点的密钥，即上文中所述的用户密钥。这个过程可以通过实际发放智能卡、也可以通过广播等来完成，或可以采用其它的方式。如果采用智能卡的方式，用户可以将该智能卡插入合适的接收设备（如机顶盒）中，然后等待接收运营商发送的 $MKCB$ 广播。这时，合法用户的子集合 S 应该改变为 $S'=S+A$ ，这里， A 代表新用户的节点。

当有新的用户加入时，子集差的划分产生了改变。同时，应该为新的 S' 和 MK' 生成新的 $MKCB$ ，这里 MK' 可以是新的授权密钥，也可以是原来的授权密钥 MK 。当新的 $MKCB$ 代替了原来的 $MKCB$ 时，该新用户就成功地加入了这个系统中。

在多个用户加入到该系统的情况中，与上面的过程是相同的。唯一的差别是 $S'=S+A'$ ，这里 A' 是表示所有新用户节点的集合。

如果一个用户想退出系统，或其设备发生泄密或被非法侵入的故障时，就应该将该用户从系统中移除。在这种情况下，所有合法用户的集合 S 应变为 $S'=S-A$ ，这里， A 代表这个用户的节点。

当用户退出该系统时，子集差的划分也发生了改变。应该为新的 S' 和 MK'

生成新的 MKCB, 这里, MK' 应该是新的授权密钥, 而不能是原来的旧的授权密钥。当新的 MKCB 代替了原来的 MKCB 时, 该用户就被成功地从这个系统中移除了。

5 在多个用户从该系统移除的情况中, 与上面的过程是相同的。唯一的差别是 $S'=S-A'$, 这里 A' 是表示所有被移除用户的节点的集合。

对于离开系统的用户, 该系统可以采用以下方法来停止其观看经加密的视频节目的权利: (1) 发送消息关闭该用户对 MKCB 的接收功能, 并更换现有合法用户集合 S 中的授权密钥 MK; (2) 停止向该用户发送含有授权密钥 MK 的媒体密钥控制块 MKCB。

10 对于刚刚加入系统的新用户, 由于其已经具有对应于该节点位置的各个子集差 $D(u, v)$ 的用户密钥 $K(u, v)$, 因此他们在接收到媒体密钥控制块 MKCB 后, 都可以对其进行解密从而获得授权密钥 MK。

15 另外, 用户加入到系统或从系统中被移除 (离开), 是通过该用户是否履行了注册手续 (例如是否已经交费) 为触发条件的。该系统可以自动对这种情况进行检测, 并自动计算变化后的子集差 $D(u, v)$ 、进行发送或停止发送媒体密钥控制块 MKCB。

子树算法的分析结果

20 如果集合 $(I-S)$ 具有 r 个节点, 即如图 4 所示的空白叶节点数是 r , 用数学归纳法可以证明: 子集合 S 是不大于 (2^r-1) 个子集差的并集。还可以用概率统计公式计算得到平均是 r 每增加 1, 期望的子集差的数值增加 $2\ln 2$, 大约为 1.38。因此子集差的平均值大约是 $2r\ln 2$, 即 $1.38r$ 。如果 r 很大, 这个期望的数值将减小。在图 5 的示例中可以看出, $r=11$, 子集合 S 可以被分割为的子集差最多是 21 个, 符合上述算式 $2 \times 11 - 1 = 21$ 。

25 很显然, 如果子集合 S 具有 m 个节点, 则子集合 S 所需要的子集差不会超过 m 个, 因为每个子集差至少可以覆盖一个节点。一般情况下, 这个估计可以被大大减少, 因为每个子集差都可以覆盖许多节点。这说明本方法即使在最差的情况下也不会比逐节点加密发送信息更差。

30 另外, 在本发明的方法中, 对子集合 S 的覆盖是用子集差 $D(u, v)$ 来完成的, 这样做在大多数情况下子集差的个数会比较小, 但本发明并不限于此, 还可以采用其它方法, 比如说直接用子集 $T(u)$ 来覆盖。

直接用于集来覆盖的优点是用户需要存储的用户密钥比较少, 每个用户

都只需要存储 n 个密钥即可。但是其缺点也很明显，比如当只需要废除一个用户的时候，整个二叉树就会被分成 $n-1$ 个子集，其代价相对于子集差覆盖（在该种情况下仅需一个子集差）来说显然要大得多。

5 本发明也可以考虑一般的树结构，不仅是二叉树，也可以是三叉树或多叉树。在一般的树结构中也可以考虑用直接子集覆盖的方法，以及子集差覆盖的方法。

另外，本发明也不限于使用子树的方法，还可以使用其它方法完成如本发明中对用户的多层分组，并使该分组的情况随着有效用户的增加或减少而实际地改变，从而减少 MKCB 中所含有的消息的长度。

10 MKCB 方法的优点

与常规的 CA 系统相比，MKCB 方法有两个主要的优点：

15 首先，根据子树算法，MKCB 的长度比传统的 EMM 的长度大大缩短。MKCB 的长度依赖于在对子集合 S 的分割中的子集差的数量。在很少用户从系统中移除的情况下，或在子集合 S 的树结构很“干净（即树结构中的节点位置相对集中和整齐）”，MKCB 的长度比传统的线性 EMM 要短很多，而该传统线性 EMM 的长度是与用户的数量成线性正比的。MKCB 能够被实现得越短，就能节省更多的带宽。

20 其次，在常规的 CA 系统中，用户的移除将使同组中的其他用户改变为新组，其中保证其他用户正确地改变他们的组是非常重要的，但是要达到此目的，就要花费大量的带宽加密所要发送的信息。在本发明中，由于 MKCB 非常短，其广播和分配的时间和形式十分灵活，当从系统中移除用户时，不用将其他用户分配为新的组，因此对其他用户的影响非常小。

25 上面对本发明的实施例进行了详细地说明。本领域的普通技术人员应该明白，按照本发明的精神及指导思想对本发明做出的各种修改都在本发明后附的权利要求书所要求保护的范围内。

说明书附图

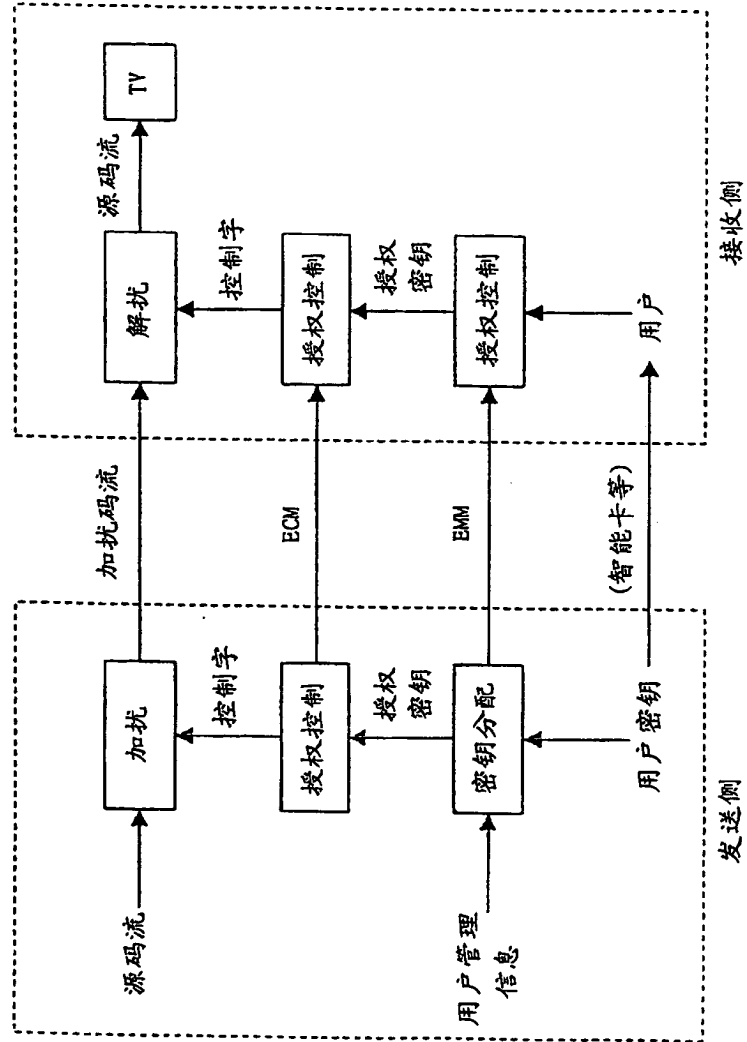


图 1

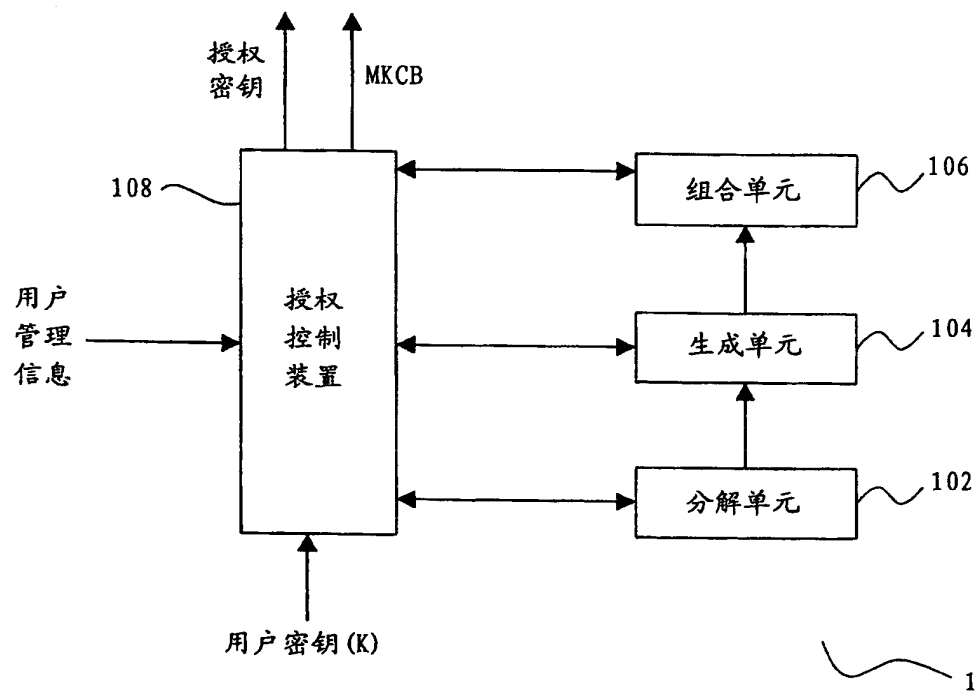


图 2

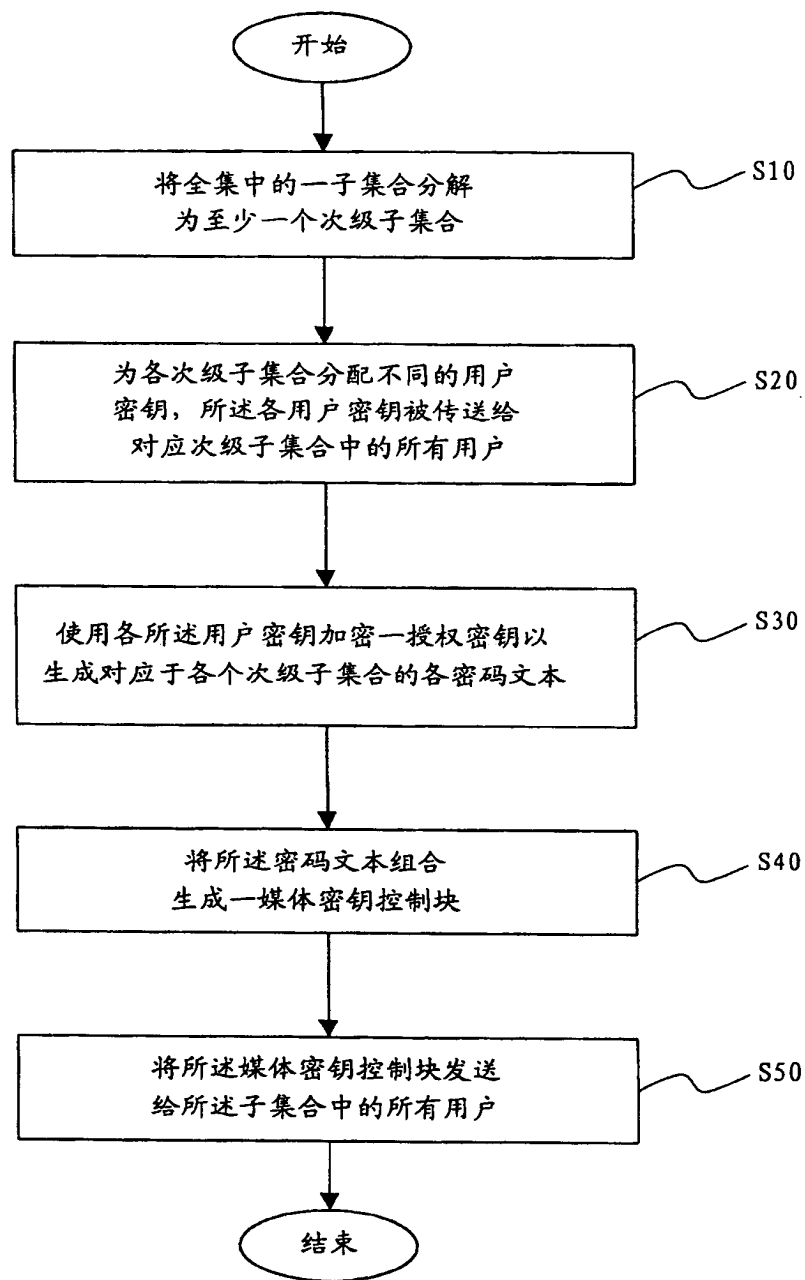


图 3

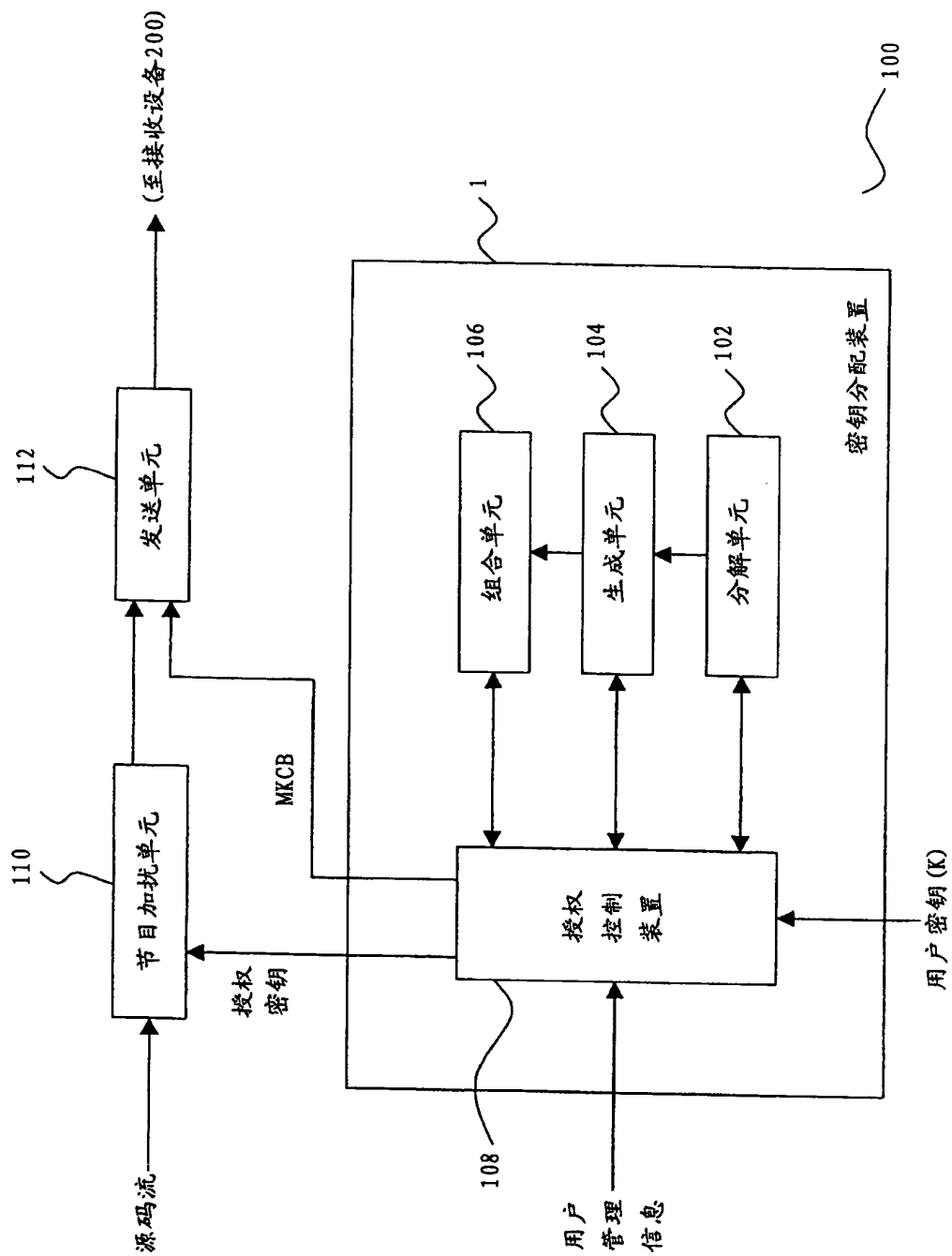


图 4

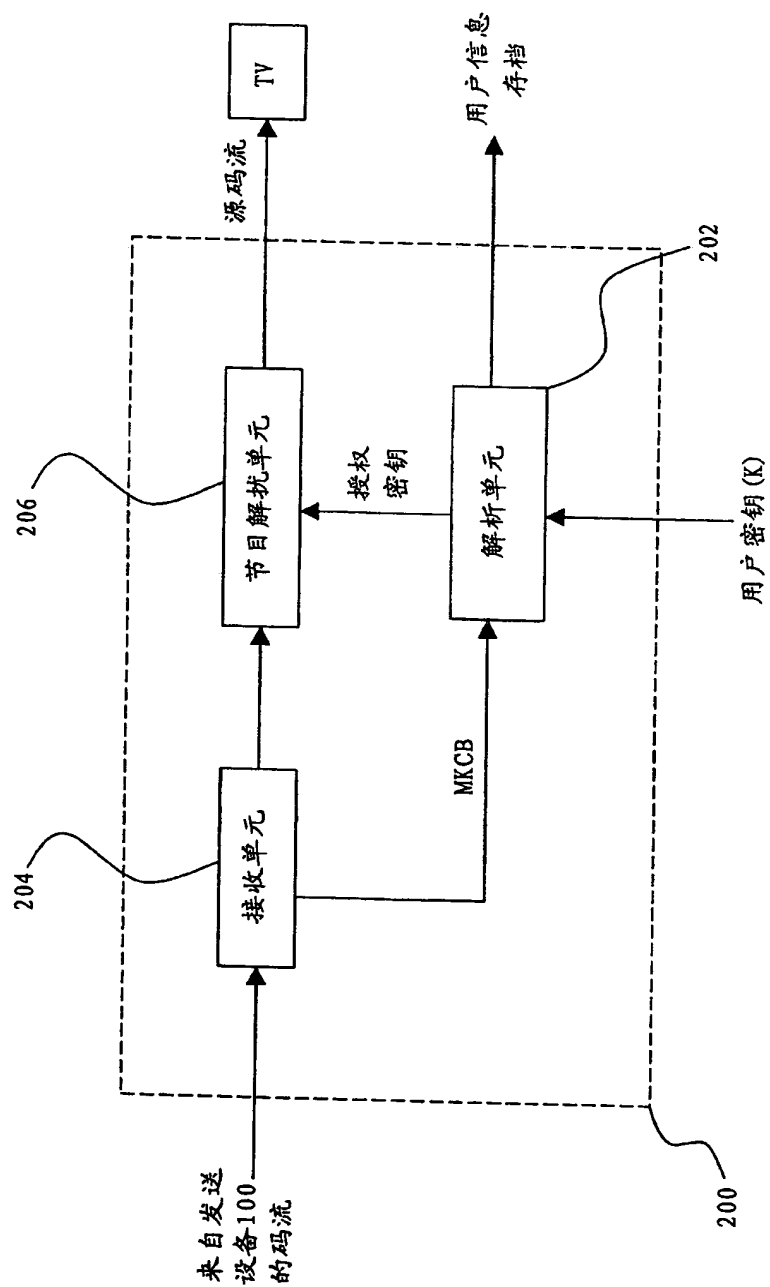


图 5

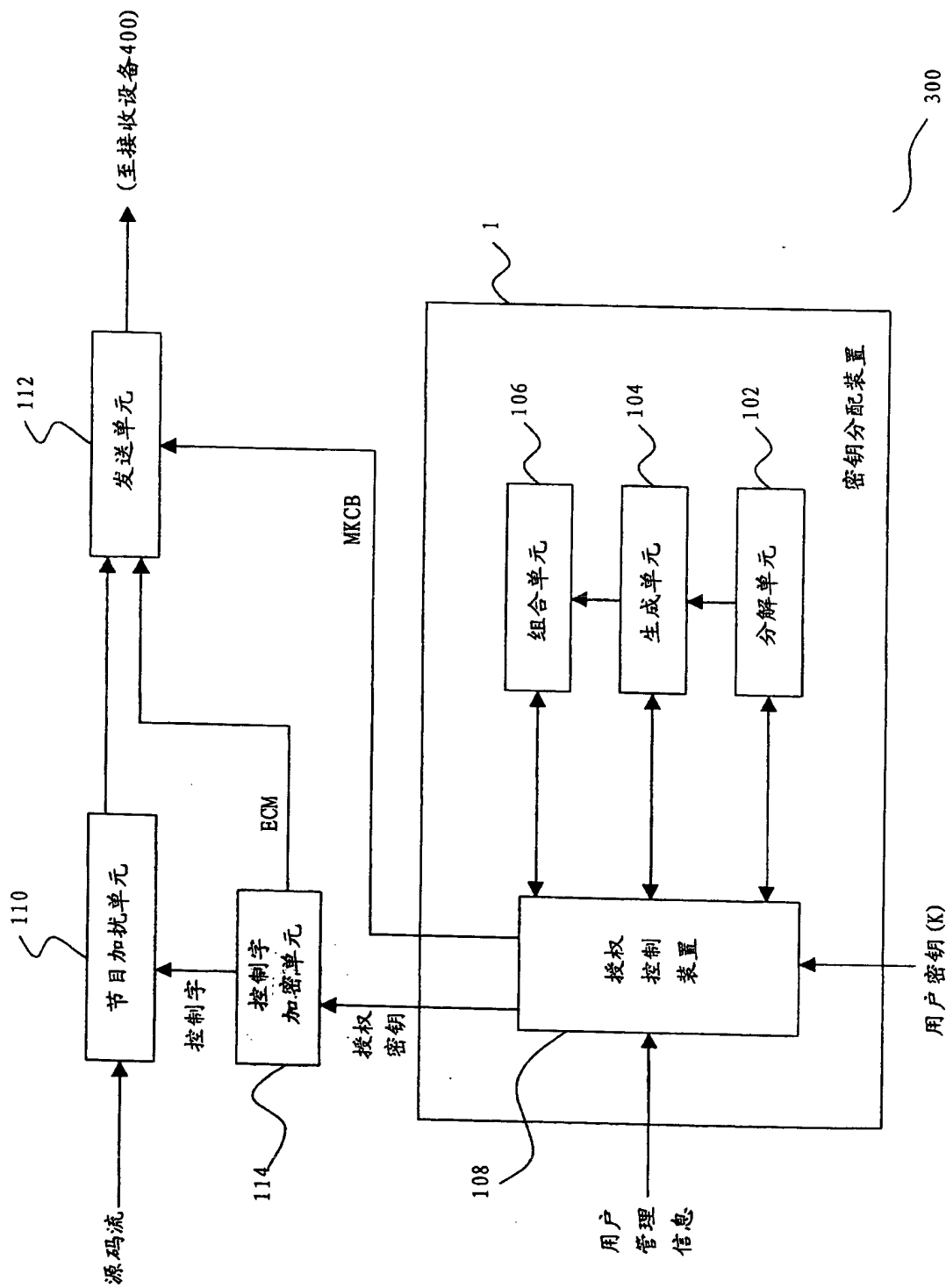


图 6

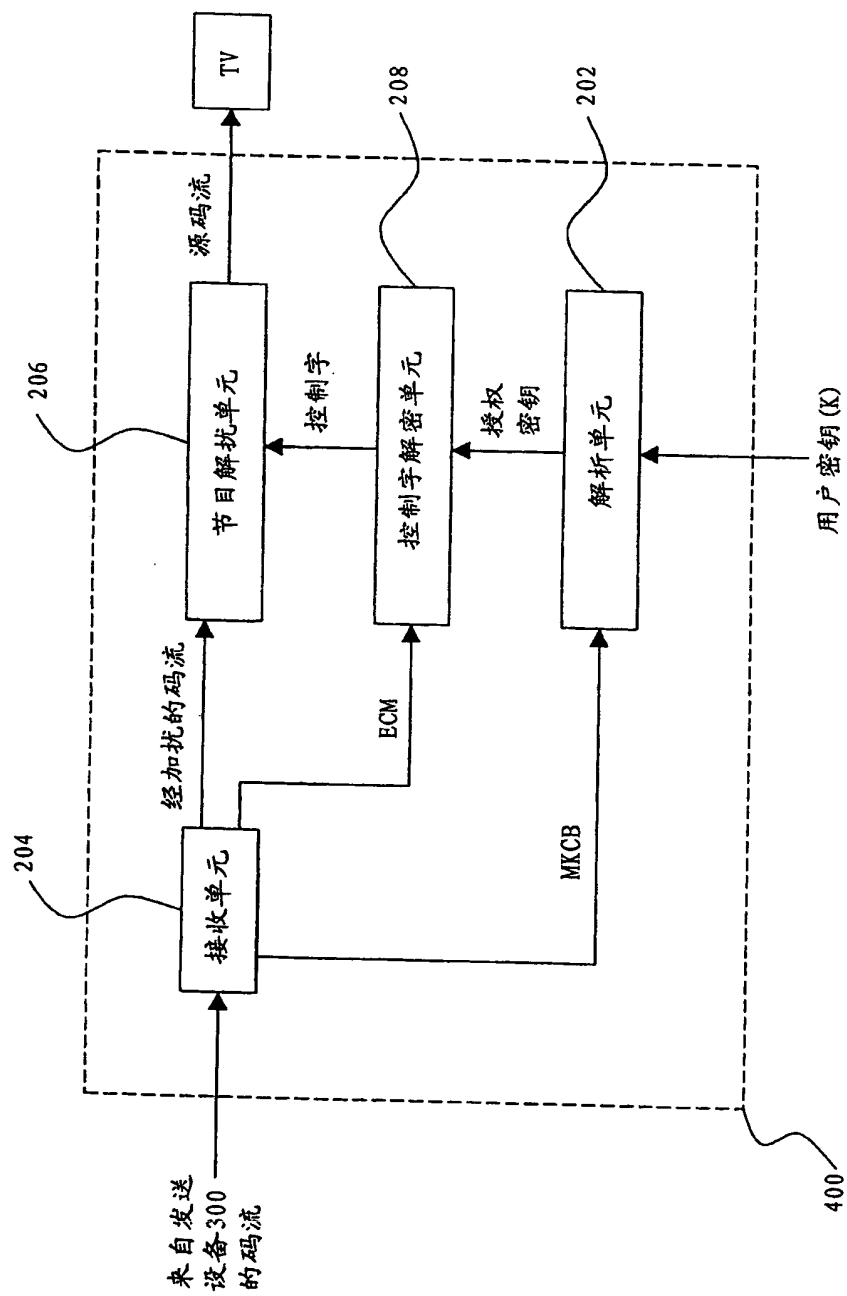
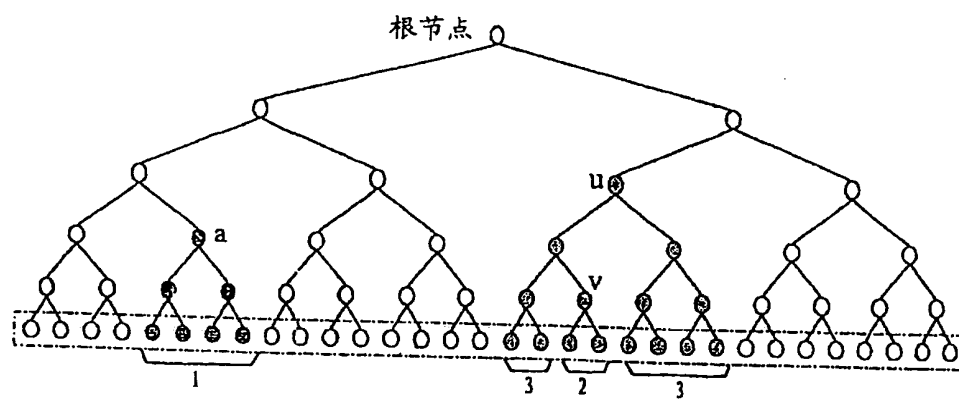
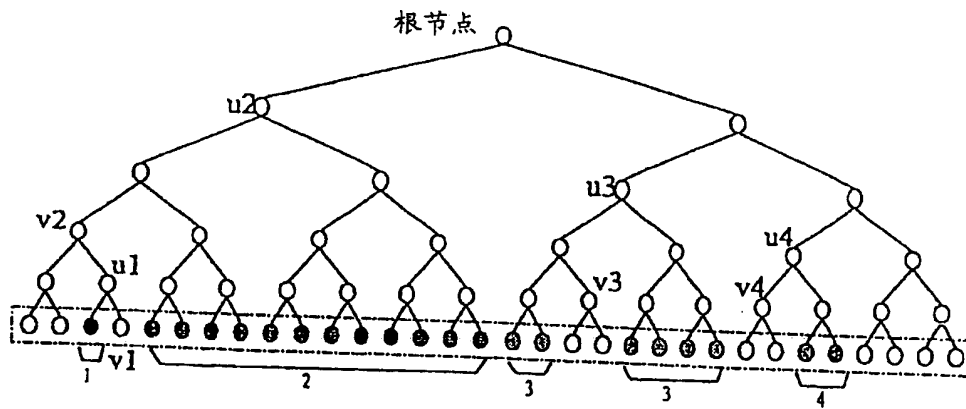


图 7



- 1 与节点a 相关的子树
- 2 与节点v 相关的子树
- 3 由 $D'(u, v)$ 识别的子树差

图 8



- 1 子集差 $D(u1, v1)$
- 2 子集差 $D(u2, v2)$
- 3 子集差 $D(u3, v3)$
- 4 子集差 $D(u4, v4)$

图 9